

escrypt

SECURITY. TRUST. SUCCESS.

White paper

Developing and retrofitting

E/E architectures to obtain type approval

Using AUTOSAR to achieve UNECE-compliant cybersecurity



Evidence that a vehicle is appropriately protected against cyberattacks will soon be a prerequisite for type approval. One necessary condition for this is proof of an appropriate level of security based on a certified cybersecurity management system (CSMS). During development of the vehicle type, critical elements must be identified and appropriate protective measures implemented. The same applies to existing architectures; by 2024, these must also be retrofitted with appropriate protection to obtain type approval in line with UNECE WP.29.

AUTOSAR can play an important role in building the impetus required to achieve this. AUTOSAR Classic and AUTOSAR Adaptive already offer a range of useful security modules. This white paper shows exactly where, and to what extent, AUTOSAR security modules can be specifically used to implement the mitigations prescribed by Annex 5 of the UN Regulation 155.



Table of contents

Tight timeframe requires viable implementation strategy	4
Appropriate, verifiable cybersecurity through development or retrofitting	5
AUTOSAR as a key element in creating secure E/E architectures	7
Using AUTOSAR security modules for UNECE-compliant mitigation	9
Summary: Harnessing the potential of AUTOSAR security modules for type approval	11

Tight timeframe requires viable implementation strategy

With WP.29's adoption of UN Regulations Nos. 155 and 156 in June 2020, the issue of product security has become a key technology in the digitalization strategies pursued by automotive manufacturers and suppliers. In order to continue to obtain approval for their vehicle types in the EU, Japan, and other important markets, OEMs will need to operate a certified cybersecurity management system (CSMS) and demonstrate an appropriate level of IT security for their E/E architectures.

The EU is planning to make these approval requirements mandatory for new vehicle types by July 2022 and to extend them to legacy architectures by July 2024. Japan and Korea are working on similar timeframes (Fig. 1). Accordingly, car manufacturers worldwide – with the involvement of their suppliers – are faced with the task of designing, implementing, and verifying corresponding protective measures for their vehicles [1, 2].

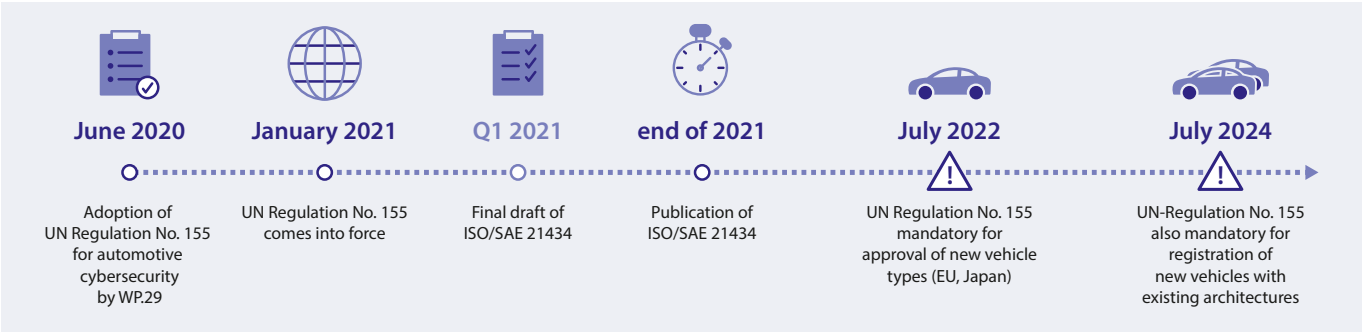


Figure 1: Timeline for UN Regulation No. 155 (UN R155): appropriate cybersecurity will be a mandatory requirement to obtain approval for new vehicle types from July 2022 and for existing architectures from July 2024.



Appropriate, verifiable cybersecurity through development or retrofitting

According to UN R 155, OEMs wishing to obtain type approval in the future will have to prove that they applied their CSMS during the development process. Even if the CSMS was not yet operational during development (prior to July 2024), the OEM must demonstrate an appropriate level of security for the vehicle type: in other words, the OEM must identify the vehicle type's critical elements and protect them from previously defined threats with appropriate security measures. Annex 5 of UN R 155 provides guidance here by listing the vulnerabilities and the threats that need to be taken into account (Part A) as well as specifying technical measures for their mitigation (Parts B, C). Accordingly, type approval is most likely to be successful if the OEMs follow a comprehensive and transparent approach that, at the very minimum, answers the following questions [1]:

1. Are all necessary artifacts available to prove that the vehicle type was developed in line with the CSMS/appropriate security measures?

OEMs must ensure seamless traceability of all the documents that prove the CSMS was applied during development (e.g. risk analyses, IT security concepts, security test specifications, and corresponding test reports). Many of these activities have long since become standard in the automotive industry. The challenge, however, is to deliver complete documentation of the measures taken to ensure the cybersecurity of the vehicle type.

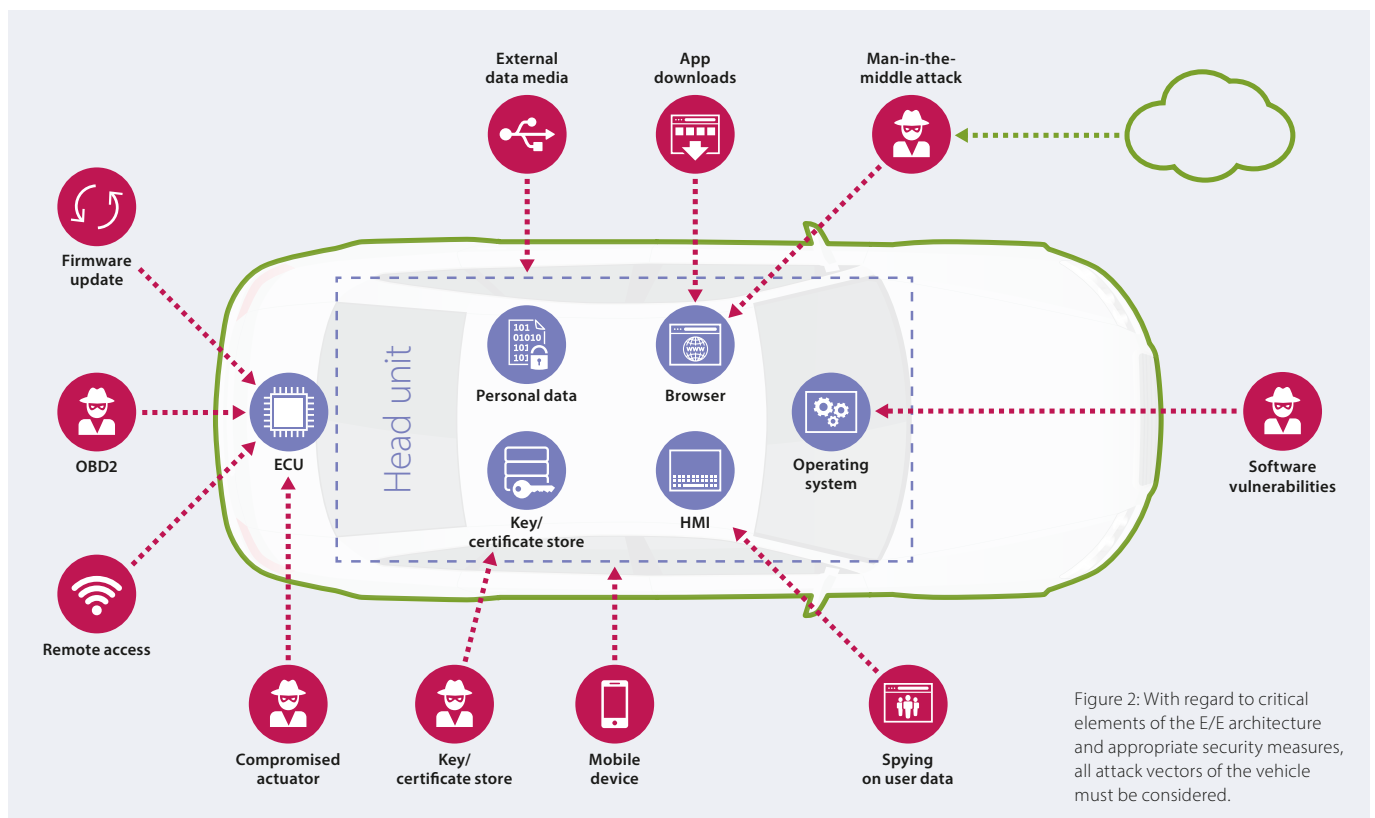


Figure 2: With regard to critical elements of the E/E architecture and appropriate security measures, all attack vectors of the vehicle must be considered.

For vehicle types developed in line with a CSMS, the required proof and documentation will come straight from the cybersecurity management system. However, the same task must also be carried out for legacy systems from July 2024 onwards: in these cases, it may be necessary to return to a time prior to the introduction of a CSMS when a defined security engineering process was in place.

2. What are the critical elements of the E/E architecture?

The best way to answer this question is to focus solely on the development and retrofitting of the vehicle type. This will help avoid budget and engineering bottlenecks as the July 2024 deadline approaches. It is also important to remember that the sooner the question of critical security elements is answered in the development cycle, the less rework will ultimately be required. Performing a readiness check before commencing any development/retrofit activity enables intelligent decisions to be made in this respect: applying the right measures at the E/E level (e.g. using AUTOSAR security modules) can reduce the effort required as compared to a purely component-centric approach.

ESCRYPT's vehicle type approval (VTA) readiness assessment systematically identifies potentially critical elements by drawing on examples from the official UN R 155 interpretation document, feedback from technical services, and over a decade of experience in analyzing and designing secure vehicle architectures (Fig. 2). A key part of the readiness assessment is the identification of technical security gaps; this, in turn, paves the way for initial budget estimates, relevant IT security checks, and the prioritization of tasks on the path to type approval.

3. Which technical cybersecurity measures, both at the ECU and E/E level, have been implemented and why are they appropriate – especially with regard to Annex 5?

The third decisive step toward type approval is to define and implement the necessary technical measures to establish appropriate cybersecurity for the vehicle. Sections 7.3.3 and 7.3.4 of UN R 155 require the vehicle manufacturer to:

- conduct a risk assessment of the vehicle type with regard to the various vehicle systems and their interaction with each other and with external systems, and
- provide proof of what appropriate protective measures have been taken to mitigate the identified risks (in accordance with Annex 5, Parts B and C, and, if necessary, beyond).

Accordingly, during development of the vehicle type, the OEM must implement those IT security components and mechanisms that guarantee appropriate security of the E/E architecture at the time of type approval – both in the architecture's individual systems as well as in how those systems communicate with each other and with the outside world.

This third aspect – the implementation of appropriate security measures in accordance with Annex 5 – represents a particular challenge for existing architectures, which must be ready to meet mandatory approval requirements as of July 2024. These architectures will potentially require the retrofitting of legacy hardware and software components. In this case, it may prove to be very advantageous if the components include AUTOSAR security modules, because these can be used as levers to minimize the time and cost of retrofits.

AUTOSAR as a key element in creating secure E/E architectures

In view of the growing range of threat scenarios and the increasing number of attack vectors in connected vehicles, UNECE WP.29 makes type approval dependent on whether the threats and security measures listed in Annex 5 of the regulation have been demonstrably taken into account in the vehicle's development. This is a demanding task when viewed simply from a technical perspective – but even more so when the time horizon is so tightly constrained. At the moment, vehicle manufacturers are still in the process of putting in place the necessary organizational and process-related prerequisites in the form of a CSMS – yet they must already start implementing the required mitigating IT security mechanisms in the E/E architecture for new vehicle types that will be ready for approval in less than two years.

But this is only part of the challenge. While new vehicle types can be developed in a manner that allows them to be approved from the outset in line with UNECE requirements and the CSMS, it is also necessary to modernize existing architectures, for which no security processes were originally envisioned under UNECE WP.29, in order to prepare them for type approval from 2024. However, it can sometimes be difficult to retrospectively implement state-of-the-art security for these existing architectures.

AUTOSAR security modules

An obvious solution is to rely primarily on known technologies and standards. As a widely used, proven software platform for developing E/E architectures, AUTOSAR is the natural means to an end here – not just for developing new architectures, but also for retrofitting existing ones. This is because the standardized specifications in AUTOSAR have long since taken IT security into account. Both AUTOSAR Classic and AUTOSAR Adaptive already have a number of IT security modules. These, in turn, can be translated directly into functional security within the vehicle electrical system architecture and can be specifically employed in the spirit of “security by design” to implement several of the mitigations prescribed by UNECE WP.29 [1, 3, 4]:

■ **Crypto stack**

In AUTOSAR, the targeted provision of cryptographic keys and certificates is carried out by the crypto stack (crypto API). Irrespective of the crypto implementation, the applications access only the interfaces provided by the crypto stack, thus increasing the portability of applications to different ECUs.

■ **Secure communication**

With secure onboard communication (SecOC), AUTOSAR offers a communication protocol that protects data traffic on standard vehicle buses such as CAN and allows a granular adjustment of security levels. AUTOSAR Adaptive also supports TCP/IP communication via Ethernet using TLS and IPSec, thus facilitating the establishment of secure connections not only within the vehicle, but also with external instances such as the OEM backend.

■ **Secure diagnostics / logging:**

AUTOSAR also monitors authorized access to sensitive data in the vehicle network using the UDS services 0x27 (security access) and 0x29 (authentication). For example, the diagnostic test apparatus gains access to such data only if it has previously carried out a challenge-response communication or authenticated itself using a certificate. In addition, AUTOSAR supports the logging of security-relevant events in the security event memory.

■ **Identity and access management**

The AUTOSAR identity and access management module ensures that only authorized applications gain access to certain critical resources (e.g. sensitive data in the persistent memory, communications channels, cryptographic keys). These access rights can be configured according to the OEMs requirements in AUTOSAR and updated at any time.

■ **Intrusion detection**

An important component of effective security management throughout the vehicle life cycle is an intrusion detection system (IDS) that detects attacks on the vehicle and reports them to a backend. For this reason, the IDS manager (IdSM) has been integrated into AUTOSAR since the R20-11 release as a crucial control point for a distributed IDS [5].

- **Secure updates**

The secure update function in AUTOSAR Adaptive then helps fix any identified vulnerabilities by receiving and processing security updates for individual applications or even for the entire platform. The individual update blobs are signed by the backend, so that only updates from trustworthy sources are executed.

- **Trusted platform**

ECU, domain controller (DCU), and vehicle computer (VC) applications must also be verified at regular intervals. This task is conducted by either secure boot or the trusted platform function in AUTOSAR Adaptive, which, as a continuation of the secure boot chain of trust, verifies the integrity of all applications as well as of the platform itself. This ensures that only trusted software is executed.

Most of the AUTOSAR security modules listed above are available for both platforms, Classic and Adaptive, but some are supported only for AUTOSAR Adaptive (Fig. 3). However, the AUTOSAR consortium takes a needs-based approach to driving development in this area. For example, plans are already in place to extend the secure update function to AUTOSAR Classic.

Retrofitting legacy systems using AUTOSAR

AUTOSAR is therefore very much a method of choice for closing gaps in existing architectures and preparing legacy systems for type approval by implementing and verifying appropriate security measures. In many ECUs based on AUTOSAR Classic, the SecOC module is either already present or can be retrofitted with little effort. This makes it relatively unproblematic to implement secure onboard communication in existing architectures, so that these architectures can continue to be approved in their further developed form.

However, retrofitting existing E/E architectures using AUTOSAR does not work in all cases: unlike SecOC, for example, which has long been an integral part of AUTOSAR in most ECUs, newer security features such as IDS and secure updates cannot be retrofitted as easily, because they are not compatible with earlier versions of AUTOSAR. Nevertheless, AUTOSAR represents a useful cornerstone for the implementation of UNECE-compliant security measures wherever upgrades of existing vehicle systems are possible – and especially when it comes to developing new E/E architectures [1].

	AUTOSAR Classic R20-11	AUTOSAR Adaptive R20-11
Crypto stack	✓	✓
Secure communication	✓	✓
Secure diagnostics / logging	✓	✓
Identity and access management	✗	✓
Intrusion detection	✓	✓
Secure updates	✗	✓
Trusted platform	✗	✓

Figure 3: Security modules in AUTOSAR Classic and Adaptive (last updated November 2020).

Using AUTOSAR security modules for UNECE-compliant mitigation

The question remains at which point, and to what extent, the security features offered by AUTOSAR can specifically help meet the individual requirements of UNECE WP.29 for the cybersecurity of the vehicle type and for the mitigation of vehicle-specific threats (in line with Annex 5, Part B). What is already clear is that the existing AUTOSAR security modules can be applied in different ways, and to varying degrees, to the specific directives of the regulatory text concerning possible vulnerabilities.

A useful next step is therefore to carry out a qualitative rating to demonstrate the different degrees to which each individual AUTOSAR security module can be applied to the individual mitigations listed in Annex 5 of the UNECE regulations (see Fig. 4 “AUTOSAR-UNECE Security Matrix” on page 10). On this basis, a distinction can then be made between the following two types of security module:

- Complementary security module: the AUTOSAR security module provides functions that support mitigation as part of a broader concept.
- Constitutive security module: the AUTOSAR security module provides features that accomplish mitigation to a high degree.

Meeting requirements with AUTOSAR modules – two examples

The table overleaf (Fig. 4, AUTOSAR-UNECE Security Matrix) provides specific information on potential attack vectors and the extent to which AUTOSAR security can be used to achieve type-approval-compliant protection of the E/E architecture. The following two examples (mitigations postulated in Annex 5, Part B) show how to interpret this table in terms of assigning and classifying AUTOSAR security modules [2]:

■ M10 – The vehicle shall verify the authenticity and integrity of messages it receives.

The authenticity and integrity of in-vehicle communication can be verified using the secure communication protocols offered by AUTOSAR. These protocols can be used practically “out of the box” (••), though they must, of course, be configured correctly [6]. Secure communication also depends on cryptographic keys and primitives, both of which are provided by the AUTOSAR crypto stack, which thus provides additional support for this use case (•).

■ M18 – Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege.

User authentication and authorization can be implemented on two different levels with AUTOSAR: the AUTOSAR secure diagnostics module can be used to authenticate access through the diagnostic tester (•), while the identity & access management module restricts the access of user-exposed applications to critical resources (•). In this example, however, the two AUTOSAR modules cover only partial aspects; they do not by any means guarantee control of all possible and conceivable forms of user access to the vehicle. As such, they do not fully meet the requirement, but are still suitable for supporting mitigation.



AUTOSAR security as part of the solution

Once again, it is important to bear in mind in this context that, as middleware, AUTOSAR provides services that can be used by a wide variety of applications. Conversely, this means that even though AUTOSAR features can be used in various ways in the vehicle architecture, they do not always target the exact use case that is needed to meet a specific requirement. Nonetheless, two important conclusions on AUTOSAR security modules can be drawn from the table in Figure 4:

- AUTOSAR provides one or more modules that can support the respective technical solution for almost every mitigation required under UN R155.
- For a considerable number of these mitigations, AUTOSAR even offers functions that can be used to meet the requirements to a large extent.

In short, AUTOSAR delivers on its promise, and its diverse security modules are fundamentally suited to addressing all mitigations required by the UNECE regulations. The degree to which they contribute to meeting UNECE cybersecurity requirements as a prerequisite for type approval – i.e. whether they meet these requirements fully or only partially – is more nuanced. In other words, AUTOSAR can certainly be an important part of the solution, but does not by itself provide the full answer. To achieve holistic vehicle security, security concepts must be developed for all mitigations – and these concepts will include both AUTOSAR modules and additional security systems such as hardware security modules (HSMs).

AUTOSAR-UNECE security matrix

 <p>Measures to be taken into account according to Annex 5 of UN Regulation No. 155</p>							
	Secure communication Crypto stack	Secure diagnostics/logging	Identity & access mgmt.	Intrusion detection system	Secure updates		Trusted platform
M3 Security controls shall be applied to back-end systems. Where back-end servers are critical to the provision of services, there are recovery measures in case of system outage.	Outside the scope of the AUTOSAR application – mitigates threats outside the vehicle						
M6 Systems shall implement security by design to minimize risks.	●	●	●	●	●	●	●
M7 Access control techniques and designs shall be applied to protect system data/code.			●	●			
M8 Through system design and access control, it should not be possible for unauthorized personnel to access personal or system-critical data.			●	●			
M9 Measures shall be employed to prevent and detect unauthorized access.				●●	●		
M10 The vehicle shall verify the authenticity and integrity of messages it receives.	●	●●					
M11 Security controls shall be implemented for storing cryptographic keys.	●						
M12 Confidential data transmitted to or from the vehicle shall be protected.	●						
M13 Measures to detect and recover from a denial of service attack shall be employed.					●		
M14 Measures to protect systems against embedded viruses/malware should be considered.					●		●
M15 Measures to detect malicious internal messages or activity should be considered.		●●		●	●		
M16 Secure software update procedures shall be employed.	●					●●	
M18 Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege.			●	●			
M19 Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions.			●	●	●		
M20 Security controls shall be applied to systems that have remote access.	●			●			
M21 Software shall be security assessed, authenticated and integrity protected. security controls shall be applied to minimize the risk from third-party software that is intended or foreseeable to be hosted on the vehicle.				●●			●●
M22 Security controls shall be applied to external interfaces.	●	●	●●*				
M23 Cybersecurity best practices for software and hardware development shall be followed.	Beyond the scope of application from a software perspective, but AUTOSAR offers guidelines on secure coding						
M24 Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data.	●			(●)**			

* Applies only to "Threat T18.3" (diagnostic interfaces)
 ** Roles/rights management through IAM planned but not yet implemented

Rating

- AUTOSAR provides features that can be used to implement mitigation as part of a broader concept
- AUTOSAR provides features that implement mitigation to a large extent

Figure 4: Mitigations according to Annex 5 of the UN Regulation 155 and the support offered by AUTOSAR security modules.

Summary: Harnessing the potential of AUTOSAR security modules for type approval

Very soon, OEMs, together with their suppliers, will have to demonstrate that their type approval processes and measures ensure appropriate security in the vehicle. This means vehicle manufacturers must make use of a certified cybersecurity management system (CSMS) during development of the vehicle type. Even now – while they are still in the process of establishing their cybersecurity management system – they must incorporate mitigating security mechanisms in line with UNECE requirements into the development of their E/E architectures.

The UNECE requirements are not only mandatory for the development of new vehicle types, but will also be extended to existing architectures as of mid-2024. Retrofitting legacy systems may actually be the greater challenge here. But, regardless of whether a project involves new development or retrofitting, the key steps toward appropriate cybersecurity as a prerequisite for type approval are complete documentation, the identification of critical elements, and the systematic implementation of security measures in line with Annex 5 of the UN Regulation 155.

In this context, AUTOSAR can be a useful anchor and an effective lever. This is because AUTOSAR already provides a whole range of security components that address, to varying degrees, the specific mitigations that must be taken into account under UN R155. It therefore makes sense to explicitly consider AUTOSAR security modules at appropriate points within the CSMS and to include them in the implementation of UNECE-compliant automotive cybersecurity. By successfully exploiting the inherent potential of existing AUTOSAR security components to address the threats and mitigations specified in the UNECE regulations, manufacturers and suppliers may save time and cut costs on the path toward creating an E/E architecture that is secure enough for type approval.

This turns AUTOSAR into a key factor in providing vehicles with sufficient protection to obtain approval. However, effective holistic automotive security, as required by UNECE WP.29, will ultimately have to extend beyond AUTOSAR – from the hardware security module (HSM) in the microcontroller and the vehicle's internal network to the OEM backend or vehicle security operations center (V-SOC), as well as along the entire supply chain and throughout the vehicle life cycle.

References

- [1] Moritz Minzlaff et al. UNECE wish meets AUTOSAR reality: Appropriate cybersecurity as a prerequisite for type approval. *Elektronik automotive*, November 2020.
- [2] UNECE World Forum for Harmonization of Vehicle Regulations: Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. Available at: <http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf>
- [3] Michael Schneider et al. AUTOSAR Adaptive: Cybersecurity included *Elektronik automotive*, December 2020.
- [4] AUTOSAR Release R20-11. You can find the latest information and specifications at: <https://www.autosar.org/standards/>
- [5] Jan Holle et al. Automotive cybersecurity – Efficient risk management for the entire life cycle of vehicles *ATZechnik*, November 2020.
- [6] Michael Schneider, Alexandre Berthold. AUTOSAR Security: A holistic approach *Whitepaper ESCRYPT*, October 2019.

Authors & contact details

Dr. Moritz Minzlaff

Senior Manager Security Consulting
Moritz.Minzlaff@escrypt.com

Marcel Rücker, M.Sc.

Security Consultant
Marcel.Ruecker@escrypt.com

Dr. Michael Schneider

Project Manager AUTOSAR Security
MichaelPeter.Schneider@escrypt.com

ESCRYPT GmbH
Ullsteinstrasse 128
12109 Berlin, Germany
Phone: +49-30-403-6919-00
info@escrypt.com

www.escrypt.com



All information provided is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and up-to-date information, there can be no guarantee that this information is as accurate as it was on the date it was received or that it will continue to be accurate in the future. No one should act upon this information without appropriate professional advice and without thoroughly examining the facts of the situation in question.
© ESCRYPT GmbH. All rights reserved.

Last updated: 03/2021